Ejercicio 2 – Políticas de seguridad. Sergio Vigil Díaz

Mi plan estratégico

Las personas encargadas de elaborar la política de seguridad informática de mi empresa deben de ser los directivos y todas las personas responsables de los departamentos, el departamento de informática y comunicación, el equipo de respuesta a incidentes, las personas que representan a los usuarios que pueden haberse visto afectados y los consultores especializados en el campo de la seguridad de la empresa.

Por otro lado, la política de seguridad debería de poder ser llevada a cabo mediante unos procesos administrativos en particular o a través de la instalación de dispositivos y herramientas. También debería de dar respuesta a lo que el personal necesita de ella y debe de poder adaptarse a la organización en cuestión, ya que no todas las políticas son válidas para todas las organizaciones y sus medidas deben de ser perfectamente medidas y detalladas. Además, tiene que definir un marco en el que queden establecidos todos los objetivos, cómo se ha llegado a la propuesta y la forma en la que se lleva el proceso de comunicación. Por otra parte, tiene que haber una correcta comunicación entre la empresa y todas las partes involucradas y se debe de revisar con frecuencia para evitar los posibles fallos o identificar sus mejoras. Asimismo, se debe tener en cuenta el entorno legal en el que se encuentran, teniendo cuidado con todas las acciones que pueden suponer un problema, por lo que habrá que revisar documentos oficiales como el Código Penal o la Ley Orgánica de Protección de Datos Personales antes de realizarla. De la misma manera, es muy importante realizar copias de seguridad de todos los datos y programas para mantener la seguridad.

Por otra parte, mi política debería de evitar la descarga de archivos o servicios ilegales, abrir archivos adjuntos de dudosa procedencia, compartir las contraseñas o accesos privados, usar recursos de la empresa para objetivos que no sean íntegramente de la compañía y visitar páginas web cuya URL sea incorrecta, que se utilicen certificados válidos en entornos seguros o realizando transacciones y comprobando que se cumple el protocolo HTTPS.

Finalmente, el plan una vez creado, no vale para toda la vida ya que, como he mencionado anteriormente, pueden surgir nuevos fallos o identificar mejoras de este, entonces habría que cambiarlo de forma periódica para evitar que quede obsoleto.